UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
201 Johnstone Court
Durham, North Carolina 27712

Case No. 1:22MJ 326 -1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
201 Johnstone Court, Durham, North Carolina 27712 as further described in Attachment A.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:
Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:
See attached affidavit incorporated by reference herein

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/M.C. Glenn Covington
Applicant's signature

M.C. Glenn Covington, Special Agent - H.S.I.
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 8/26/2022

Judge's signature

City and state: Winston-Salem, North Carolina

JOI ELIZABETH PEAKE, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MIDDLE DISTRICT OF NORTH CAROLINA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

IN THE MATTER OF THE SEARCH OF THE RESIDENCE, OUTBUILDINGS, AND APPURTENANCES LOCATED AT 201 JOHNSTONE COURT, DURHAM, NORTH CAROLINA 27712	Case No. 1:22mj326

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, M.C. Glenn Covington, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am investigating the trafficking of child sexual abuse material (CSAM) via a peer-to-peer network (BitTorrent) at an address in Durham County, North Carolina.

2. I am a Special Agent with the Department of Homeland Security (DHS), Homeland Security Investigations (HSI), currently assigned to Cary, North Carolina and have been so employed since October 2009. I am responsible for investigations involving the production, importation, advertising, receipt, and distribution of child pornography which occur in the

Eastern and Middle Districts of North Carolina. I was previously employed as a United States Postal Inspector for five years in Richmond, VA, and was responsible for child exploitation investigations involving the U.S. Mail. I have participated in over 400 child pornography investigations. I have received training in child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes through the United States Postal Inspection Service, the FBI, and the Department of Justice. I have also received specialized training from Internet Crimes Against Children (ICAC) Task Force seminars and at the Dallas, TX Advocacy Center's Crimes Against Children Training Conference.

3. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. This affidavit is made in support of an application for a search warrant to search the location described in Attachment A, the premises located at 201 Johnston Court, Durham, NC 27712 (hereinafter, the "SUBJECT PREMISES"), and to search and seize contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2)(A) and

2252A(a)(5)(B), which items are more specifically described in Attachment B of this Affidavit.

5. The information contained within this Affidavit is based on my training and experience, as well as information I have developed, and information relayed to me by other law enforcement officers including Detective Michelle Savage, Cary Police Department (CPD). Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A are located at the SUBJECT PREMISES, 201 Johnstone Court, Durham, NC 27712, within Durham County in the Middle District of North Carolina.

6. Det. Savage has been employed by CPD since 1999 and was previously employed at the Duke University Police Department for two (2) years. Det. Savage has been assigned to the CPD Detective Division for the past 14 years and has worked numerous rape and child sexual abuse cases. For the past two (2) years, Det. Savage has been responsible for investigations involving the receipt, distribution, or possession of child

pornography in violation of 18 U.S.C. § 2252A. She has conducted child exploitation investigations and participated in such investigations conducted by other agents. Det. Savage has undergone both formal and on-the-job training as it relates to child exploitation investigations.

7. The application for a search warrant, which this affidavit is offered in support thereof, is being applied for to seize contraband, instrumentalities, fruits and evidence, more particularly described in Attachment B, of violations of 18 U.S.C. § 2252A(a)(5)(B), which makes it a crime to possess child pornography and access with intent to view child pornography, and violations of 18 U.S.C. § 2252A(a)(2)(A), which makes it a crime to receive and distribute child pornography.

8. In summary, this Affidavit sets forth facts establishing probable cause to believe that within the SUBJECT PREMISES there are contraband, instrumentalities, fruits, and evidence of a subject who received, distributed, accessed with intent to view, and/or possessed via the Internet, images depicting minors engaging in sexually explicit conduct.

RELEVANT STATUTES

9. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.

a. Title 18, U.S.C. § 2252A(a)(2)(A), prohibits the knowing receipt or distribution of (a) any child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (b) any material that contains child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. Title 18, U.S.C. § 2252A(a)(5)(B), prohibits knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using

any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

10. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). Child Sex Abuse Material (CSAM) has the same meaning as child pornography.

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" refers to actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. *See* 18 U.S.C. § 2256(2)(A).

f. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device. *See* 18 U.S.C. § 1030(e)(1).

g. "Storage medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

h. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers,

video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

i. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic,

or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

l. "Internet Protocol Address" or "IP Address" is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

m. The "Secure Hash Algorithm" (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. SHA1 is the most widely used of the existing SHA hash functions and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty

exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

n. The term "GUID," as used herein, refers to the Globally Unique Identifier (GUID) identification number that may be issued by the Peer-to-Peer (P2P) software to computers offering to share files on the P2P network. A GUID is a pseudo-random number used in software applications. This GUID number is produced when some P2P software applications are installed on a computer. While each generated GUID is not guaranteed to be unique, the total number of unique keys is so large that the probability of the same number being generated twice is very small. When comparing these GUIDs, your affiant can quickly determine with a high degree of certainty that two different IP addresses that are associated with the same GUID are associated with the same computer.

o. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each

level read backwards—from right to left—further identifies parts of an organization. Examples of first level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and .edu for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the world wide web server located at the United States Department of Justice, which is part of the United States government.

p. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file

transfer logs list detailed information concerning files that are remotely transferred.

q. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

s. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), mobile telephone devices, video gaming devices, portable music players, Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

BACKGROUND REGARDING THE INTERNET/COMPUTERS AND CHILD PORNOGRAPHY

11. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer,

have personal knowledge of the operation of a computer, and have accessed the Internet since 1997. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

12. Computers and the Internet have revolutionized crimes involving child pornography. Computers serve multiple functions in connection with child pornography crimes including: a means of viewing, producing, distributing, receiving, and storing child pornography and a means of communicating with other offenders and enticing victims.

13. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an

individual accesses the Internet, the computer from which that individual initiate access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

14. Today, many computers manufactured for personal use come equipped with a camera enabling the user to produce images and videos. Thus, using computers, child pornographers are readily able to produce, or request that minor victims create child pornography. Further, images and videos created using digital cameras can easily be transferred directly to a computer. Using a scanner, computers can convert traditional non-digital

photographic images into a digital format thereby enabling the digitalization of child pornography produced using a film camera.

15. Individuals interested in the sexual exploitation of children may also use technology to target minors, interact with minors, and entice minors to produce child pornography. This is often accomplished using social networking applications such as Facebook, Instagram, Kik Messenger, Musical.ly, and LiveMe.

16. The ability of computers and electronic storage media to store large amounts of digital files makes them ideal repositories for child pornography. The capacity of these devices to store digital information has grown tremendously within the last several years enabling the storage of thousands of images and videos at very high resolutions.

17. A modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Through the Internet, a computer user can contact literally millions of other users around the world. The Internet affords collectors of child pornography multiple methods for storing, obtaining, distributing, and/or viewing child pornography in a relatively secure and anonymous fashion. These methods include, but are not limited to, email, instant messaging services, websites, social media

applications, cloud storage services, message boards, and P2P file sharing networks. These same means enable those involved with child pornography to communicate with like-minded offenders and minor victims. Even in cases where cloud storage is used, evidence of child pornography can be found on the user's computer or external media in most cases.

18. Mobile devices, hand-held computers, can transfer media through multiple methods—cellular signal, Wi-Fi, Bluetooth, and near field communication (NFC). In addition, mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with cloud storage and paired devices. For example, an individual using Google Pictures or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or "synced," with their other computer devices.

19. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email

as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, application data, temporary files, or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

20. Individuals involved in the receipt, possession, access with intent to view, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that can connect to the internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction, and prior versions can often be used until the current device is repaired or replaced.

THE USE OF PEER-TO-PEER FILE SHARING SOFTWARE TO DISTRIBUTE CHILD PORNOGRAPHY ON THE BITTORRENT NETWORK

21. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that millions of computer users throughout the world use P2P file sharing networks to share files containing music, graphics, movies, and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

22. The BitTorrent network is a publicly available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

23. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and FrostWire client program, among others. These client programs are publicly

available and typically free P2P client software programs that can be downloaded from the Internet.

24. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. This is commonly referred to as "passive distribution."

25. As an example, during the downloading and installation of the publicly available µTorrent client program, the license agreement for the software states the following: "Automatic Uploading. µTorrent accelerates downloads by enabling your computer to grab pieces of files from other µTorrent or BitTorrent users simultaneously. Your use of the µTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In µTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall µTorrent through the Add/Remove Programs control panel utility. In addition, you can control µTorrent in multiple ways through its user interface without affecting any files you have already downloaded."

26. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network can download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding."

27. Files or sets of files are shared on the BitTorrent network via the use of "Torrents." A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent." The "info hash" is a SHA1 hash value of the set of data describing the file(s) referenced in the "Torrent." This set of data includes the SHA1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers." "Trackers" are

computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part, or all of the file(s) referenced in the "Torrent." "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing.

28. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

29. To locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword

search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file.

30. It is again important to note that the actual file(s) referenced in the "Torrent" are obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the Internet Protocol (IP) addresses of the remote peers/clients. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their

computer from the website. Typically, the BitTorrent client program on their computer will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients would then be located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files to the user's computer.

31. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA1 piece hash described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

32. Law enforcement efforts have resulted in the creation of BitTorrent network client programs that obtain information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they

are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA1 hash values of torrents which have been previously identified by law enforcement as being associated with such files. The law enforcement BitTorrent network client programs allows for single-source downloads of files of child pornography or suspected child pornography from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in sharing digital files of known or suspected child pornography on the BitTorrent network. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the law enforcement BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is or are being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. The law

enforcement BitTorrent client program can log this information. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children (ICAC) Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the active sexual exploitation of actual child victims.

PROBABLE CAUSE

33. As part of undercover investigations, law enforcement agents around the country have devised several pro-active investigative techniques aimed at identifying and investigating individuals involved in the sexual exploitation of minors through the production, distribution, receipt, and possession of child pornography. One such technique is the use of P2P file-sharing software, to include the sharing of child pornography on the BitTorrent network.

34. On March 28, 2022, Det. Savage was conducting an online investigation on the BitTorrent network for offenders sharing child

pornography. Det. Savage directed the investigative focus to a device at IP address 98.26.62.136, because it was associated with a torrent with the infohash: c153780b0bb14c065aec25de3f50ed23ca2de368cc. This torrent file references 4733 files, at least one (1) of which was identified as being a file of investigative interest to child pornography investigations.

35. Det. Savage used a computer running investigative BitTorrent software. Det. Savage utilized a secure connection to directly connect to the device at IP address 98.26.62.136, hereinafter referred to as the "Suspect Device." Suspect Device reported it was using BitTorrent client software – TR 3000 – Transmission 3.00.

36. On March 28, 2022, between 12 hrs. and 1416 hrs., Det. Savage successfully completed a download of 145 files that the device at IP address 98.26.62.136 was making available. The device at IP Address 98.26.62.136 was the sole candidate for this entire download, and as such, each file was downloaded directly from this IP address. A sample of three (3) of these files are described below.

> File Name: Videos_6yo_Tiny_Tessa_Ass_Fuck_v3rtq4ykz.webm
> Hash Value: 3R7N3TZ5236A523XN4QLUWUK4JDFFYUC
> This is a color video depicting an adult male inserting the tip of his penis into a prepubescent minor female's anus.

File Name: !!_pthc_center_ptsc2014_hot_9yr.avi
Hash Value: ELIMFVL7ODVISHDHNNHKC7O46FIEK44K
This is a color video depicting naked prepubescent minor female performing oral sex on an adult male. The adult male ejaculates on the minor's face.

File name: VV102.jpg
Hash Value: 5MHIMVSICR6QEG3DYJFQFNCK755NFODV
This is a color image depicting a naked prepubescent minor male, approximately, 8- to 11-year-old, lying on his back with his legs in the air exposing his genitals and anus in a lewd and lascivious manner.

37. On April 7, 2022, Det. Savage was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Det. Savage directed the investigative focus again to the Suspect Device, a device at IP address 98.26.62.136, because it was associated with a torrent with the infohash: c6df06f418649befb76e424767c57adde8e9e391. This torrent file references 10,111 files, at least one (1) of which was identified as being a file of investigative interest to child pornography investigations.

38. Using a computer running investigative BitTorrent software, Det. Savage utilized a secure connection to directly connect to the Suspect Device at IP address 98.26.62.136. The Suspect Device reported it was using BitTorrent client software – qBittorrent/4.4.2.

39. Between April 7, 2022, at 1420 hrs. and April 8, 2022, at 0749 hrs., Det. Savage successfully completed a download of 9705 files that the Suspect Device at IP address 98.26.62.136 was making available. The device at IP Address 98.26.62.136 was the sole candidate for this entire download, and as such, the files were downloaded directly from this IP address. A sample of three (3) of these files are described below.

> File Name: IMG_3233.jpg
> Hash Value: X47HCBMJTTFNKXHC7CYL2RJ7JTBFS62H
> This is a color image depicting a prepubescent minor female who pulled her underwear to the side and exposed her genitals in a lewd and lascivious manner.
>
> File Name: IMG_8632.jpg
> Hash Value: KJQHEAGXVDJMKVQMJYP5AEWXQHDI4QFE
> This is a color image depicting a prepubescent minor female using her hands to pull apart her genitals in a lewd and lascivious manner.
>
> File Name: yarina-075.jpg
> Hash Value: SFNNGGUOWFGJSDRACXKS625SXBM5M25T
> This is a color image of a naked minor female, approximately 9 to 12-year-old, sitting on the floor with her legs spread apart exposing her genitals in a lewd and lascivious manner.

40. On April 18, 2022, Det. Savage was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. Det. Savage directed the investigative focus again to the Suspect Device at IP address 98.26.62.136, because it was associated with a

torrent with the infohash: 510a4ecf6c35ecf562e8969fadfd13470fb0a0bf. This torrent file references 6,233 files, at least one (1) of which was identified as being a file of investigative interest to child pornography investigations.

41. Using a computer running investigative BitTorrent software, Det. Savage utilized a secure connection to directly connect to the Suspect Device at IP address 98.26.62.136. The Suspect Device reported it was using BitTorrent client software – qB4420-qBittorrent/4.4.2.

42. On April 18, 2022, between 1006 hrs. and 1649 hrs., Det. Savage successfully completed a download of 65 files that the Suspect Device at IP address 98.26.62.136 was making available. The device at IP Address 98.26.62.136 was the sole candidate for this entire download, and as such, the files were downloaded directly from this IP address. A sample of three (3) of these files are described below.

> File Name: stickcam_alexis_is_a_sexy_beast.avi
> Hash Value: 6WN2SAVAFF55ZFKVDS33QKN6XE7NL27N
> This is a color video depicting a minor female, approximately 10 to 14 years, placing whipped cream on genitals and a dog licks her genitals.
>
> File Name: stickam_casseytunner_fucks_herself.avi
> Hash Value: 6QLT3QSEAAGTZW567GNGG07EM42RWAQX
> This is a color video depicting a minor female, approximately 11- to 14-year-old, spreading apart her genitals and then inserts her hand/fingers in her genitals.

File Name: Hxc-baby_girl123 selfmade vib (15 y0)-stickam Webcam PT.avi
Hash Value: KDCX4DP4UA0AXRD6LKWL50SH4HY3RRTU
This is a color video depicting a minor female, approximately 13- to 16-year-old, inserting a hairbrush into her genitals.

43. On April 19, 2022, a query was made on the IP address 98.26.62.136 through the American Registry for Internet Numbers (ARIN). ARIN reported IP address 98.26.62.136 to be registered to Charter Communications, Inc.

44. A Department of Homeland Security Investigations (HSI) summons was served on Charter Communications, Inc. for the subscriber utilizing the IP address 98.26.62.136 on March 28, 2022, at 12:15:00 UTC – 14:16:00 UTC PM, April 7, 2022, at 14:20:00 UTC – April 8, 2022, at 07:49:00 UTC, and April 18, 2022, at 10:06:00 UTC – 16:49:00 UTC. As a result of the summons, Charter Communications, Inc. provided the following account information[1]

Subscriber Name: ADAM PERRYMAN

[1] A review of the Charter Communications, Inc. return shows the first date and time requested in the subpoena, March 28, 2022, at 12:15:00 UTC, and the last date and time requested in the subpoena, April 18, 2022 16:49:00 UTC, listed for the IP address 98.26.62.136 as the target details from the return. Although the return did not specifically list the other dates and times requested in the subpoena between the first and last dates, the IP address was assigned to Adam Perryman at the SUBJECT PREMISES during that time as described below.

Account Number:	276524903
Service Address:	201 JOHNSTONE COURT, DURHAM, NC 27712
User Name:	9105406913@CHARTER.NET
Phone Number:	9105406913

45. Charter Communications, Inc. provided the IP address history for 98.26.62.136. According to the returns received from Charter Communications, Inc., the IP address 98.26.62.136 was assigned to Adam PERRYMAN at the SUBJECT PREMISES from December 15, 2020, until at least April 23, 2022.

46. According to a search of the North Carolina Division of Motor Vehicles records your affiant conducted on or about August 10, 2022, Adam Jehu PERRYMAN, date of birth of June 14, 1977, Stephanie Perryman, date of birth January 8, 1971, and Mary Peoples, date of birth October 7, 1944, reside at 201 Johnstone Court, Durham, NC 27712 (SUBJECT PREMISES).

47. Your affiant conducted a search of public records via ACCURINT to obtain information relating to the SUBJECT PREMISES. ACCURINT, which is owned and operated by LexisNexis, Inc., is an information database service that is sold commercially to U.S. law enforcement agencies for legitimate investigations. The search of ACCURINT records indicated that

Adam Jehu PERRYMAN, Stephanie Perryman, and Mary Peoples reside at the SUBJECT PREMISES.

48. On August 10, 2022, a representative of the United States Postal Inspection Service informed your affiant that the last name of PERRYMAN and Peoples are receiving mail at the SUBJECT PREMISES.

49. On August 9, 2022, your affiant observed the residence located at the SUBJECT PREMISES. The residence is a two-story single-family white brick residence with black shutters. The front door is white with a window in the middle of the door and glass panels on either side of the front door. On the left side of the residence is a two (2) car garage. At the end of the concrete driveway on the left-hand side is a green mailbox affixed to white a post. On the side of the mailbox is "201 Johnstone Court."

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

52. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of

children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard

copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such

correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Based on the repeated offering of child pornography for download by others through his BitTorrent downloads, and his steady building of an apparent collection of child pornography over time, as evidenced by the child pornography that Det. Savage was able to download from the Suspect Device, the user of the computer at the SUBJECT PREMISES has demonstrated conduct consistent with the behavior of collectors of child pornography as discussed above.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

52. As described in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in

whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

53. *Probable cause.* I submit that if a computer or storage medium is found at the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

54. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record

information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can

indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein

may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on

a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

55. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media,

and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software

available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the SUBJECT PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

56. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

57. Because several people may share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain storage

media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

PROCEDURE FOR UNLOCKING ENCRYPTED DEVICES

58. The search warrant requests authorization to use the biometric unlock features of a device (including phones and computers), as described in Attachment B, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices (including phones and computers). To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress Adam Jehu PERRYMAN's, Stephanie PERRYMAN's, and Mary PEOPLES's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of Adam Jehu PERRYMAN's, Stephanie PERRYMAN's, and Mary PEOPLES's face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.

CONCLUSION

59. Based on the aforementioned information, I respectfully submit that there is probable cause to believe that contraband, evidence, fruits, and instrumentalities of offenses in violation of 18 U.S.C. § 2252A, as more fully

described in Attachment B of this Affidavit, may be located at the residence described in Attachment A.

59. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES and the seizure of the items listed in Attachment B to include a full forensic examination of any computers, electronics, and related devices listed here.

/s/ M.C. Glenn Covington
M.C. Glenn Covington
Special Agent
Homeland Security Investigations

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of the written affidavit.

8/26/2022

HON. JOI ELIZABETH PEAKE
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The entire property located at 201 Johnstone Court, Durham, NC 27712, including the residence, any outbuildings, and other structures on the premises, and any appurtenances thereto (all which constitute the SUBJECT PREMISES).

The residence is a two-story single-family white brick residence with black shutters. The front door is white with a window in the middle of the door and glass panels on either side of the front door. On the left side of the residence is a two (2) car garage. At the end of the concrete driveway on the left-hand side is a green mailbox affixed to white a post. On the side of the mailbox is "201 Johnstone Court". See below photographs.

ATTACHMENT B

PROPERTY TO BE SEARCHED AND/OR SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored, which then may be search for the items set out below.

2. Routers, modems, and network equipment used to connect computers to the Internet.

3. Child pornography, as defined in 18 U.S.C. 2256(8).

4. Child erotica.

5. Records, information, and items relating to violations of the statutes described above in the form of:

   a. records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);

   b. records and information referencing child erotica;

   c. records, information, and items referencing or revealing the occupancy or ownership of 201 Johnstone Court, Durham, NC 27712 including utility and telephone bills, mail envelopes, or addressed correspondence;

   d. records and information referencing or revealing the use of peer-to-peer software, including BitTorrent client software;

   e. records and information revealing sexual interest in minors;

   f. records and information referencing or revealing trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

g. records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

h. records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography; and

i. records and information revealing the use and identification of remote computing services such as email accounts or cloud storage.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing

history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

h. records of or information about Internet Protocol addresses used by the COMPUTER;

i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child sexual exploitation content.

7. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers,

notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

During the execution of the search of the SUBJECT PREMISES described in Attachment A, law enforcement personnel are also pecfically authorized to compel Adam Jehu PERRYMAN, Stephanie PERRYMAN, and Mary PEOPLES, if present at the time of the execution of the warrant, to provide biometric features, including pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:

a. any of the DEVICES found at the SUBJECT PREMISES, and

b. where the DEVICES are limited to which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as

described in the search warrant affidavit and warrant attachments,

for the purpose of attempting to unlock the DEVICES' security features in order to search the contents as authorized by this warrant, but only if Adam Jehu PERRYMAN, Stephanie PERRYMAN, and Mary PEOPLES are present at the time of the execution and the process is carried out with dispatch in the immediate vicinity of the SUBJECT PREMISES.

This warrant does not authorize law enforcement personnel to compel any other individuals found at the SUBJECT PREMISES to provide biometric features, as described in the preceding paragraph, to access or otherwise unlock any DEVICE. Further, this warrant does not authorize law enforcement personnel to request that any individuals present at the SUBJECT PREMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES, including by identifying the specific biometric characteristics (including unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.